Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-6, 10-12, 16-22, and 40-46 are pending in the application, with claims 1, 16, and 40 being the independent claims. Claims 7-9, 13-15, and 23-39 were previously cancelled without prejudice to or disclaimer of the subject matter recited therein. Claims 1-3, 10-12, 16, 17, and 40-46 are sought to be amended for clarity. Support for these amendments is found at least at, for example, paragraphs [0017], [0021] - [0027], [0030], [0031], [0042] - [0047] and [0065] and FIGs. 1-3, 7A, and 7B of the instant specification. These changes are believed not to introduce any new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

On page 2 of the Office Action, claims 1-6, 16, 20-22, and 40-43 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Adobe Acrobat 5.0 as described in "Adobe Acrobat 5.0 User's Guide for Chambers" (hereinafter "Acrobat") in view of U.S. Patent Publication No. 2002/0077985 to Kobata *et al.* ("Kobata") in view of U.S. Patent Publication No. 2002/0052981 to Yasuda ("Yasuda") and further in view of U.S. Patent Publication No. 2002/0178271 to Graham *et al.* ("Graham").

Applicant submits that the applied references, singly, or in the allegedly obvious combination do not describe each and every element as set forth in independent claims 1, 16, and 40.

For example, claims 1, 16, and 40 as amended herein recite, *inter alia*:

> determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key.

On pages 3 and 4 of the Office Action, claims 16 and 40 were rejected based on the same rationale applied to claim 1. Claims 16 and 40 recite a method and a computer readable medium, respectively with distinguishing features similar to claim 1.

Applicant submits that the applied references, in the sections cited by the Examiner, or in other sections, contain no teaching or suggestion of at least the above-noted distinguishing features of claims 1, 16, and 40.

The Examiner acknowledges that Adobe as modified by Kobata and Yasuda fails to disclose "requiring a file key obtained by an authenticated user to access the protected file." (Office Action, page 3). Rather, the Examiner relies on Graham to cure the deficiencies of Adobe as modified by Kobata and Yasuda. The Examiner states, which Applicant does not acquiesce to, that Graham "teaches requiring a file (decryption) key obtained by an authenticated use[r] to access a file" in paragraph [0066] and that "it would have been obvious to a person of ordinary skill in the art to use the Kobata et al. method of preventing clipboard operations for secure documents to prevent copying from a secured PDF to an unsecured Word [P]erfect document and ... receiving a copy command, storing the designated content to the clipboard application and then determining whether the content can be used and to require a user to be authenticated to obtain a key to gain access." (Office Action, pages 3 and 4).

Applicant respectfully disagrees with the Examiner's characterization of Graham. Graham describes a "proxy file management system" wherein "[p]rior to requesting a file, the user preferably authenticates with authentication system", "[a]fter authentication, when an end-user requests a file, the proxy system obtains verification of the authentication of the user from the authentication system and in cooperation with the policy system, the proxy system determines if the requesting user has the right to access the file" (Graham, paragraphs [0020] - [0022] and [0064] - [0066]). In Graham's system, "[i]f access to the file is granted, the proxy system provides the file, in a secure and encrypted manner, with additional information (e.g., usage rights and encryption/decryption keys) to the end-user client device." (Graham, paragraph [0022]). However, Graham does not teach or suggest "wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key", as recited in amended claims 1, 16, and 40. In contrast to the above-noted distinguishing features of claims 1, 16, and 40, Graham describes that "[i]f ***access to the file is granted***, the proxy system 110 provides the file, in a secure and encrypted manner, ***with additional information (e.g., usage rights and encryption/decryption keys)*** to the end-user client device 150." (Graham, paragraph [0066]) (emphasis added). Thus, Graham grants access to a file separate from "usage rights and encryption/decryption keys" and does not disclose that the file includes a header having a file key available to an authenticated user, wherein the secured file cannot be accessed without the file key. Moreover, Graham is limited to providing an encrypted file with usage rights and encryption/decryption file keys after granting access, via an end-user client device, to the file based upon successful verification and authentication of a requesting user. Graham fails to disclose, teach, or suggest wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key. In Graham's system, after granting access to a file, a proxy file management system provides an encrypted file with access rights and encryption/decryption keys. Graham's system provides encrypted files with encryption/decryption keys only after both verifying the authentication of the user from the authentication system and determining if the requesting user has the right to access the file (Graham, paragraph [0066]). In contrast, claims 1, 16, and 40 recite "determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key" without Graham's limitations of requiring preliminary authentication and user rights determination. Graham may discuss "a dynamic content management system (DCMS)" that "modifies the operating system of a computer to detect and "hook" different types of files based on their header information" and "provides provisions for modifying the header information of a computer file" (Graham, paragraphs [0024]-[0026]). However, Graham fails to teach or suggest the above-noted distinguishing features of claims 1, 16, and 40.

The Examiner states that Acrobat discloses determining whether the source file is a secured file because "requiring a password to access a document makes [the document] secure and the determining step must be performed in order to know whether to ask for a password" (Office Action, page 3). Even assuming for the sake of argument that the Examiner's conclusory statement is correct, which Applicant does not acquiesce to, Acrobat fails to teach or suggest "determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key", as recited, using respective language, in claims 1, 16, and 14. Acrobat may describe that "[u]sers can set passwords to prevent others from viewing, editing or printing certain documents

... during the editing process" and that Adobe Acrobat PDF format files can be password protected (Acrobat, pages 28 and 29). However, as acknowledged by the Examiner, Acrobat fails to disclose "preventing subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is the secured file" and "preventing subsequent storage of the designated content to a second destination application via the clipboard application in response to determining that the source file is the secured file" as recited, using respective language, in claims 1, 16, and 40 (Office Action, page 3).

Yasuda does not cure the acknowledged deficiencies of Acrobat. Although Yasuda describes that "the copy suppress processing part 53 determines whether or not to suppress copying of data" by referring "to the definition file 4 to determine whether or not the clipboard canceller is set to "ON"" (Yasuda, paragraph [0138]), the clipboard canceller disclosed in Yasuda is not analogous to a file key available to an authenticated user as recited in claims 1, 16, and 40. In contrast to the above-noted distinguishing features in claims 1, 16, and 40, Yasuda describes that "the system manager sets a clipboard canceller to suppress or allow the copy operation by the user", "[the system manager] sets "ON" to the clipboard canceller in order to suppress copying of data through a clipboard, or the system manager sets "OFF" to the clipboard canceller in order to allow to copy data through the clipboard", and "saves a setting of the clipboard canceller to the definition file" (Yasuda, paragraphs [0130] and [0131]). Applicant submits that Yasuda's clipboard canceller feature is limited to a user-selected (i.e., system manager-selected) binary "ON" "OFF" setting that is saved in a definition file. Yasuda further describes that the system manager's selections are made on a per-application basis in order to suppress or allow application menu items and functions

(Yasuda, paragraphs [0053]-[0059] and [0066] and FIGs. 1 and 3). Thus, Yasuda's selections are not made on a per-source file basis. Therefore, Yasuda fails to disclose, teach, or suggest determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key, as recited in claims 1, 16, and 40. The deficiencies of Acrobat and Yasuda are not cured by Kobata. Kobata is not stated to teach or suggest, nor does Kobata teach or suggest, at least the above noted distinguishing features of claims 1, 16, and 40.

Moreover, on page 3 of the Office Action the Examiner concedes that Acrobat does not disclose preventing subsequent usage and storage of the designated content in a second destination application via the clipboard application in response to determining that the source file is the secured file, as recited in claims 1, 16, and 40. Rather, the Examiner relies on Kobata and Yasuda to cure the acknowledged deficiencies of Acrobat.

Kobata and Yasuda do not cure the deficiencies of Acrobat with regards to claims 1, 16, and 40.

On pages 3 and 4 of the Office Action the Examiner asserts, which Applicant does not acquiesce to, that Kobata "teaches preventing cut/paste (i.e., clipboard) operations from being used to copy a protected document into another application" and that "Yasuda teaches receiving a copy command, storing the designated content and then determining whether the content can be used" and that "it would have been obvious to a person of ordinary skill in the art to use the Kobata et al. method of preventing clipboard operations for secure documents to prevent copying from a secured PDF to an unsecured Word [P]erfect document and to [receive] a copy command, [store] the designated content and then determining whether the content can be used." Applicant respectfully disagrees with the Examiner's assertions.

Yasuda does not teach or suggest the capability of determining or receiving a copy selection associated with designated content of a source file being displayed by a first source application, as recited, using respective language, in claims 1, 16, and 40. Yasuda generally describes a system wherein a computer operating system (OS) "transfers data at a copy-from to the clipboard" after "the user conducts a paste instruction for pasting the data copied" (Yasuda, paragraphs [0132]-[0142]). Yasuda may describe that "when the data transferred into the clipboard is cleared" and "the clipboard canceller in the definition file 4 is set to "ON"" "the original data at the copy-from cannot be copied (can be prohibited or suppressed)" or "when the clipboard canceller in the definition file 4 is set to "OFF", the original data at the copy-from is copied to the copy-to since the data transferred from the copy-from to the clipboard is not cleared (a normal copy operation via the clipboard is conducted)" (Yasuda, paragraph [0142]). However, Yasuda does not define what is meant by a "copy-from" and Yasuda does not teach or suggest at least, preventing subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is the secured file, as recited in claims 1, 16, and 40.

Instead of the above-noted distinguishing features of claims 1, 16, and 40; Yasuda is limited to performing data transfers by an OS to a clipboard after "the user conducts a copy operation for copying data on the display unit of the user terminal." (Yasuda, paragraph [0134]). Applicant respectfully submits that the Examiner has mischaracterized the teachings of Yasuda. An OS data transfer from a display of a user terminal is not analogous to determining or receiving a copy selection associated with designated content of a source file being displayed by a first source application, as recited, using respective language, in claims 1, 16, and 40.

Although Yasuda "prohibit[s] copying of data through the clipboard" by suppressing copying of data and replacing "data with empty data in the clipboard" (Yasuda, paragraphs [0132]-[0139] and [0142]) and suppresses copying of data through a clipboard by suppressing the display of an application menu item (Yasuda, paragraphs [0011], [0012], [0045], and [0143] and FIGs. 1-3), Yasuda does not teach or suggest receiving or determining a copy selection associated with designated content of a source file being displayed by a first source application, as recited, using respective language, in claims 1, 16, and 40. In contrast to the above-noted distinguishing features of claims 1, 16, and 40; Yasuda prohibits copying of data by clearing content of a clipboard when the notice for copying data is detected and copying "the content (actually no data) in the clipboard" (Yasuda, paragraphs [0016], [0017] and [0048]).

Acrobat, Kobata, Yasuda, and Graham, alone or in the allegedly obvious combination do not teach or suggest preventing subsequent storage of the designated content in a second destination application via the clipboard application in response to determining that the source file is the secured file.

While Kobata may describe how "digital content 1805 being viewed with the viewer 1820 (e.g., in a partial window on a computer screen) is prevented from being copied and pasted to another application" (Kobata, paragraph [0222]), Kobata does not teach or suggest determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key, as recited, using respective language, in claims 1, 16, and 40. In contrast to what is recited in independent claims 1, 16, and 40; Kobata discloses that "digital content 1805 being viewed with the viewer 1820 (e.g., in a partial window on a computer screen) may be prevented from being copied and pasted to another application" and that viewer 1820 is limited to "manipulating the digital content once authorization to manipulate the digital content 1805 is determined", "may be particular to the type of digital content 1805 being controlled", and "may perform ... authorization, identification, digital rights modification and decryption procedures as necessary" (Kobata, paragraphs [0214] and [0222]). In contrast to storing designated content to a clipboard application, as recited in claim 1; Kobata's system stores "digital content" in an "electronic virtual warehouse" or in the memory of a computer device (Kobata, paragraphs [0089] and [0098]).

Therefore, Yasuda, Kobata, and Graham do not cure the acknowledged deficiencies of Acrobat, and cannot be used to establish a *prima facie* case of obviousness. Thus, the allegedly obvious combination of Acrobat, Kobata, and Yasuda does not teach or suggest each and every limitation of claims 1, 16, and 40.

For at least these reasons, independent claims 1, 16, and 40 are allowable over the applied references. Reconsideration and allowance of these claims is respectfully requested.

Claims 2-6 and 10-12, which depend upon claim 1, are allowable for at least being dependent from allowable independent claim 1, in addition to their own respective distinguishing features. See *In Re Fine*, 837 F.2d 1071 (Fed. Cir. 1988) and M.P.E.P. § 2143.03.

At least based on their respective dependencies upon independent claim 16, claims 17-22 should be found allowable, as well as for their additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and remove the rejections of claims 1-6, 16, 20-22, and 40 under 35 U.S.C. § 103(a) and pass these claims to allowance.

On page 6 of the Office Action, claims 44-46 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Acrobat as modified by Kobata, Yasuda, and Graham, and further in view of U.S. Patent No. 7,281,272 to Rubin *et al.* ("Rubin"). Applicant traverses this rejection for the reasons stated below.

As noted above with regards to claim 1, the allegedly obvious combination of Acrobat, Kobata, Yasuda, and Graham does not teach or suggest each and every feature of claim 1. In particular, the combination of Acrobat, Kobata, Yasuda, and Graham does not teach or suggest determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key. Rubin is not stated to teach or suggest, nor does Rubin teach or suggest, at least the above noted distinguishing features of claim 1. Rubin is directed to "protecting digital images from being copied from a video [random access memory] RAM" (Rubin, col. 3, lines 56-57) and is silent regarding the above-noted distinguishing features of claim 1. Claims 44-46 depend from claim 1, and therefore the combination of Acrobat, Kobata, Yasuda, Graham, and Rubin does not render claims 44-46 obvious for at least the same reasons discussed above with regards to claim 1, and further in view of their own respective features.

Applicant therefore respectfully requests that the rejection of claims 44-46 under 35 U.S.C. § 103(a) be reconsidered and withdrawn.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn Perry

Glenn J. Perry
Attorney for Applicant
Registration No. 28,458

Date: 2 Dec. 2009

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

1016920_2.DOC